DDoS攻撃への備え

今回は、2010年7月から9月に発生したインシデントに関する報告とともに、小規模システムでのDDoS攻撃への備え、クラウドコンピューティング等の共用システムにおけるセキュリティの検討と、デジタルフォレンジックの概要を取り上げます。

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2010年7月から9月までの期間では、前回に引き続きWebブラウザとそのプラグインに関係する複数の脆弱性が悪用されました。また、SIPを悪用して有償の通話を行うことで金銭被害を及ぼす事件が発生したことに続き、9月には社会情勢に応じて日本国内の複数のWebサーバに対する同時多発的な攻撃が発生しました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

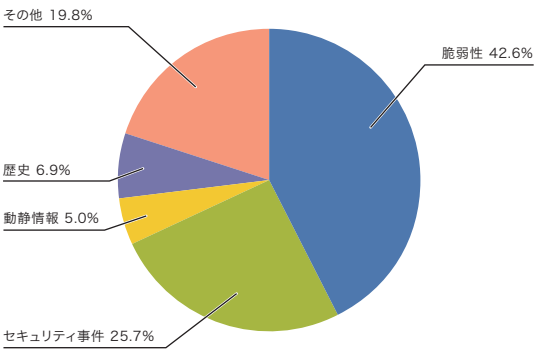


図-1　カテゴリ別比率(2010年7月～9月)

1.2 インシデントサマリー

ここでは、2010年7月から9月までの期間にIIJが取り扱ったインシデントと、その対応を示します。この期間に取り扱ったインシデントの分布を図-1に示します*1。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のWindowsを対象とした脆弱性*2*3*4*5と、アドビ社のAdobe ReaderとAcrobat*6*7、Flash Player*8*9、アップル社のQuickTime*10等のアプリケーションに数多くの脆弱性が発見され、修正されています。これらの脆弱性のいくつかは、対策が公開される前に悪用が確認されました。また、Linux kernelにおいても脆弱性*11が修正されています。さらに、DNSサーバのBIND*12やDHCPサーバであるISC DHCP*13といったサーバアプリケーション、シスコシステムズ社のCisco IOS等のルータ製品でも複数の脆弱性*14*15が修正されています。加えて、携帯電話等のファームウェアとして利用される、アップル社のiOS*16においても脆弱性が修正されています。

■ 動静情報

IIJは、国際情勢や時事に関連する各種動静情報にも注意を払っています。今回対象とした期間では、9月初旬に発生した中国の船舶による海上保安庁の巡視船への衝突行為等に注目しました。

＊1　このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットやユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃等、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策等の作業が該当する。
セキュリティ事件:ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中等、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

＊2　マイクロソフトセキュリティ情報MS10-042-緊急ヘルプとサポートセンターの脆弱性により、リモートでコードが実行される (2229593)（http://www.microsoft.com/japan/technet/security/bulletin/ms10-042.mspx)。

＊3　マイクロソフトセキュリティ情報MS10-046-緊急Windows シェルの脆弱性により、リモートでコードが実行される (2286198)（http://www.microsoft.com/japan/technet/security/bulletin/ms10-046.mspx)。

■ 歴史

この期間には、過去に歴史的背景によるDDoS攻撃やホームページの改ざん事件が発生したことがあります。今回は、9月18日（満州事変の日）に攻撃予告の情報があり、IIJの設備やIIJのお客様のネットワークに対する攻撃行為に注意を払いました。本件に関連した攻撃により、複数の政府官公庁関連組織や、一般の企業、事件とは関係ない団体のWebサイト等に対し、DDoS攻撃や改ざんの試みが発生しました。

■ セキュリティ事件

動静情報に結びつかない突発的なインシデントとしては、シーメンス社製の産業用制御システム[*17]を標的として活動を行うマルウェアが発見[*18]されています。また、以前から発生しているSIPの不正な通信の増加が確認[*19]されています。さらに、Twitterにクロスサイトスクリプティング脆弱性[*20]が発見され、悪用[*21]されたり、広告配信サーバの脆弱性を悪用し、一部のデータを改ざんしてスケアウェアへ誘導する事件[*22]も発生しています。

■ その他

その他セキュリティに関係する動向としては、DNSSECの導入に関して、DNSの最上位階層であるルートゾーンへの署名が実施[*23]され、日本でも2011年1月にJPドメイン名サービスにおけるDNSSECを導入することが発表[*24]されました。また、TLSのrenegotiation機能に関係するプロトコルの脆弱性に伴って規定されたRFC5746を実装した修正プログラム[*25]が、マイクロソフト社から提供されました。さらに、9月には毎日未修正の脆弱性を発表する試みが行われ、実際に多くの脆弱性情報が公開されました[*26]。

＊4　マイクロソフトセキュリティ アドバイザリ（2269637）安全でないライブラリのロードにより、リモートでコードが実行される（http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx）。
＊5　マイクロソフトセキュリティ情報MS10-070-重要ASP.NETの脆弱性により、情報漏えいが起こる（2418042）（http://www.microsoft.com/japan/technet/security/bulletin/ms10-070.mspx）。
＊6　APSB10-17 Adobe ReaderとAcrobatに関するセキュリティ情報（http://www.adobe.com/jp/support/security/bulletins/apsb10-17.html）。
＊7　APSB10-21 Acrobatおよび Adobe Readerセキュリティアップデーターの公開（http://kb2.adobe.com/jp/cps/871/cpsid_87135.html）。
＊8　APSB10-16 Flash Player用セキュリティアップデート公開（http://www.adobe.com/jp/support/security/bulletins/apsb10-16.html）。
＊9　APSB10-22 Flash Playerに関するセキュリティアップデート公開（http://www.adobe.com/jp/support/security/bulletins/apsb10-22.html）。
＊10 QuickTime 7.6.7のセキュリティコンテンツについて（http://support.apple.com/kb/HT4290?viewlocale=ja_JP）。
＊11 JVNDB-2010-002118 64-bitプラットフォーム上で稼働しているLinux kernelのcompat_alloc_user_space関数における権限昇格の脆弱性（http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-002118.html）。
＊12 RRSIG query handling bug in BIND 9.7.1（http://www.isc.org/software/bind/advisories/cve-2010-0213）。
＊13 DHCP: Fencepost error on zero-length client identifier（http://www.isc.org/software/dhcp/advisories/cve-2010-2156）。
＊14 Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerability（http://www.cisco.com/JP/support/public/ht/security/109/1091094/cisco-sa-20100827-bgp-j.shtml）。
＊15 Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 22, 2010（http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml）。
＊16 iPhoneおよびiPod touch用のiOS 4.1のセキュリティコンテンツについて（http://support.apple.com/kb/HT4334?viewlocale=ja_JP）。
＊17 SCADA: Supervisory Control And Data Acquisitionの一種。コンピュータによるシステム監視とプロセス制御を行う監視制御システムで、主に工場等で利用されている。
＊18 このマルウェアに関する詳細報告は複数あるが、例えば次は日本シーサート協議会による解説。マルウェア Stuxnet（スタクスネット）について（http://www.nca.gr.jp/2010/stuxnet/index.html）。
＊19 不正なSIP着信 24（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+24）。cNotesでは不定期にSIPに関する観測情報が提供されている。
＊20 この脆弱性については次の公式blogに詳しい。Twitterブログ「マウスオーバーの」問題についての全容（http://blog.twitter.jp/2010/09/blog-post_22.html）。
＊21 この件についての詳細は次のエフセキュアブログに詳しい。「Twitter.com」に放たれたワーム（http://blog.f-secure.jp/archives/50446597.html）。
＊22 この事件については次のトレンドマイクロ株式会社の Blogでも紹介されている。Adobe製品へのゼロデイ攻撃、広告配信システムを通じた「Webからの脅威」－2010年9月の脅威動向を振り返る（http://blog.trendmicro.co.jp/archives/3700）。
＊23 ルートゾーンへの署名導入に関する報告（http://www.root-dnssec.org/2010/07/16/status-update-2010-07-16/）。
＊24 JPRSによるサービス案内JPドメイン名サービスへのDNSSECの導入予定について（http://jprs.jp/info/notice/20090709-dnssec.html）。
＊25 TLS renegotiation機能に関する修正は次の更新プログラムに含まれている。マイクロソフト セキュリティ情報 MS10-049-緊急SChannelの脆弱性により、リモートでコードが実行される（980436）（http://www.microsoft.com/japan/technet/security/bulletin/ms10-049.mspx）。この問題に関しては本レポートVol.6（http://www.iij.ad.jp/development/iir/pdf/iir_vol06.pdf）の「1.4.2 SSL及びTLSのrenegotiation機能の脆弱性を利用した中間者攻撃」にて解説している。
＊26 MOAUB (Month of Abysssec Undisclosed Bugs)。この試みで発表された脆弱性については次のAbysssec Security Research blogにまとめられている。MOAUB - Day by Day(http://www.abysssec.com/blog/2010/09/moaub-1/)。

1.3 インシデントサーベイ

IIJでは、インターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的な調査研究と対処を行っています。ここでは、そのうちDDoS攻撃と、ネットワーク上でのマルウェアの感染活動、Webサーバに対するSQLインジェクション攻撃の実態について、その調査と分析の結果を示します。

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっています。DDoS攻撃の内容は、状況により多岐にわたります。しかし、一般には、脆弱性等の高度な知識を利用した攻撃ではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることで、サービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2010年7月から9月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。

ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模（回線容量やサーバの性能）によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*27]、サーバに対する攻撃[*28]、複合攻撃（1つの攻撃対象に対し、同時に数種類の攻撃を行うもの）の3つに分類しています。

この3ヵ月間でIIJは、622件のDDoS攻撃に対処しました。1日あたりの対処件数は6.76件で、平均発生件数は前回のレポート期間に比べて3倍に増加しました。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が1%、サーバに対する攻撃が72%、複合攻撃が27%でした。これは、9月10日から9月30日までの期間に、複数のWebサーバへの攻撃数が大幅に増加したためで、この3週間に発生した攻撃は全体の46%を占めています。

今回の対象期間で観測された最も大規模な攻撃は、回線容量に対する攻撃に分類したもので、最大27万5千ppsのパケットによって1.4Gbpsの通信量を発生させるものでした。また、攻撃の継続時間は、全体の66%が攻撃開始から30分未満で終了し、20%が30分以上24時間未満の範囲に分布しています。最も長く継続した攻撃は12日間（291時間）にわたり、最大で12万ppsのパケットにより670Mbpsの通信量を発生させた複合攻撃でした。

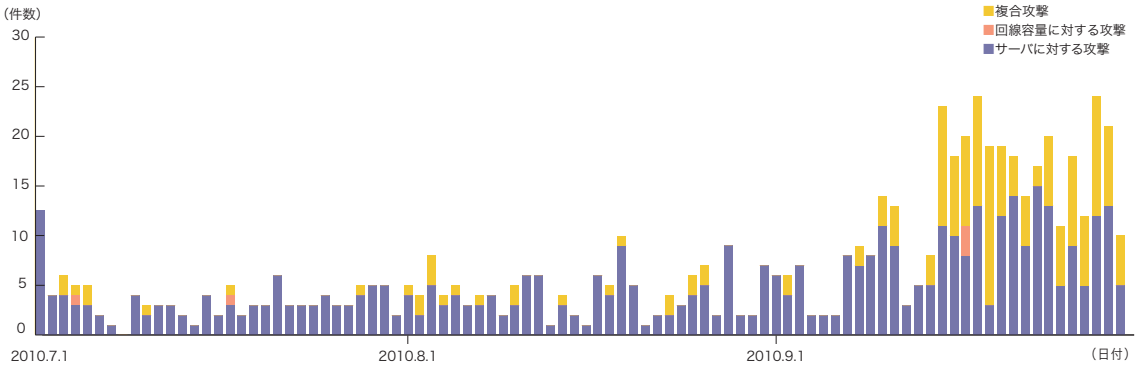


図-2 DDoS攻撃の発生件数

＊27 攻撃対象に対し、本来不必要な大きなサイズのIPパケットやその断片を大量に送りつけることで、攻撃対象の接続回線の容量を圧迫する攻撃。UDPパケットを利用した場合にはUDP floodと呼ばれ、ICMPパケットを利用した場合にはICMP floodと呼ばれる。

＊28 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃等。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリ等を無駄に利用させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立したのち、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*29]の利用や、DDoS攻撃を行うための手法としてのボットネット[*30]の利用によるものと考えられます。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*31]によるDDoS backscatter観測の結果を示します[*32]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2010年7月から9月の期間中に観測されたbackscatterについて、ポート別のパケット数推移を図-3に、発信元IPアドレスの国別分類を図-4に示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、全期間における全パケット数の58.4%を占めています。また、リモートデスクトップで利用される3389/TCPへの攻撃も観測されています。これらに加えて、5218/TCP、5224/TCP等、一般的なアプリケーションで利用されないポートも多く観測されました。図-4で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、中国の44.8%と米国の29.5%が比較的大きな割合を占めており、日本国内のIPアドレスも2.1%を占めていました。また、特に多数のbackscatterパケットが観測された、8月20日の5224/TCPと9月19日の5218/TCPを対象ポートとするパケットは、すべて中国の同一IPアドレスが攻撃対象となっています。

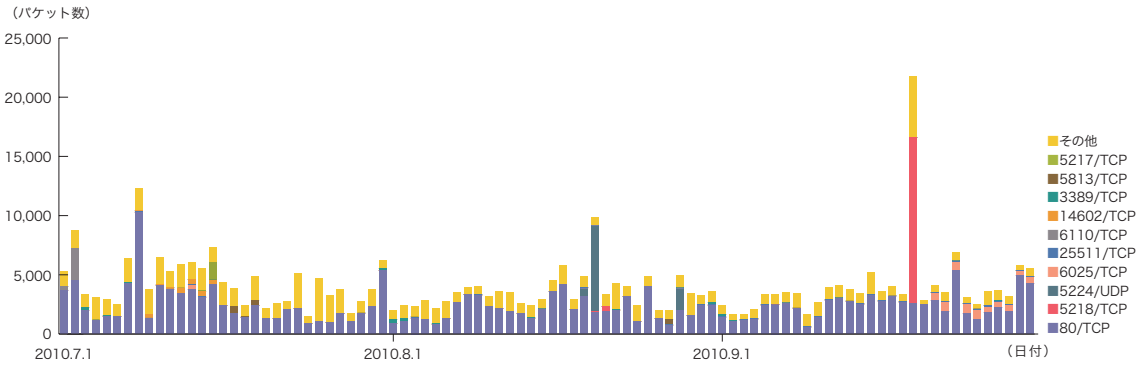


図-3　DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

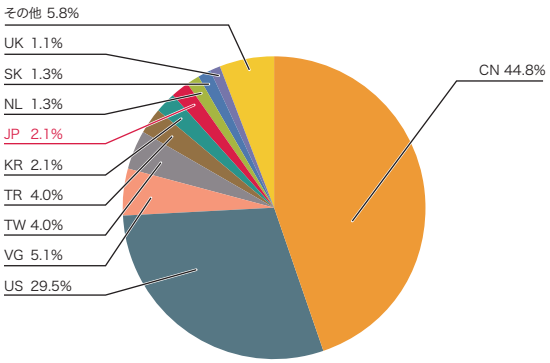


図-4　backscatter観測によるDDoS攻撃対象の分布（国別分類、全期間）

＊29 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、発信すること。

＊30 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

＊31 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。「1.3.2 マルウェアの活動」も参照。

＊32 この観測手法については、本レポートのVol.8（http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf）の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*33]による観測結果を示します。MITFでは、一般利用者と同様にインターネットに接続したハニーポット[*34]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

■ 無作為通信の状況

2010年7月から9月の期間中に、ハニーポットに到着した通信の総量（到着パケット数）の推移を図-5に、その発信元IPアドレスの国別分類を図-6にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均をとり、到着したパケットの種類（上位10種類）ごとに推移を示しています。

ハニーポットに到着した通信の多くは、マイクロソフト社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPや、telnetで利用される23/TCPに対する探索行為も観測されています。これらに加えて、5121/TCP、31795/TCP、23502/TCP、9415/TCP等、一般的なアプリケーションでは利用されない目的不明な通信も観測されました。 図-6で発信元の国別分類を見ると、日本国内の30.4%、中国の15.9 %、台湾の6.0%が比較的大きな割合を占めています。

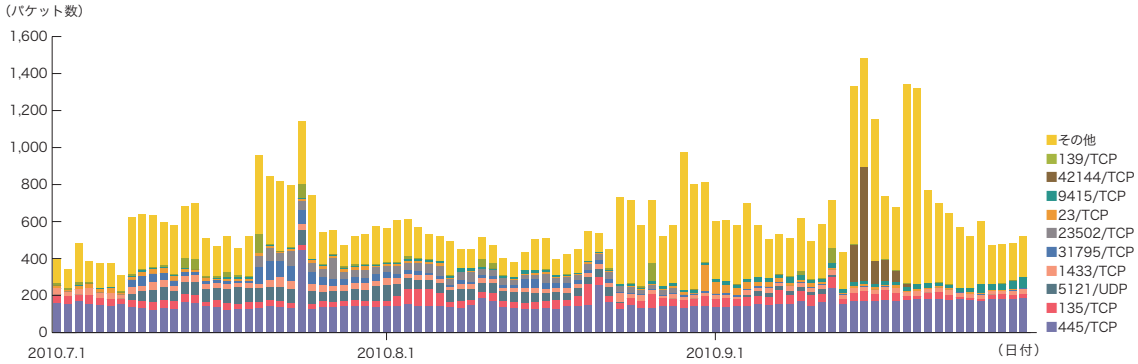


図-5　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

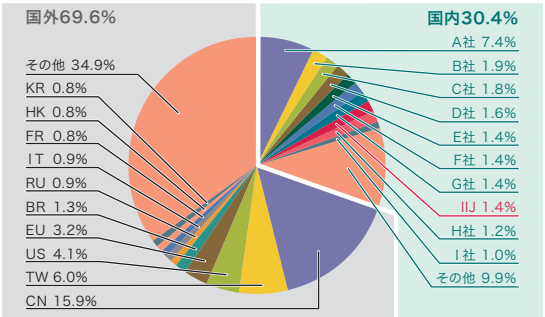


図-6　発信元の分布（国別分類、全期間）

＊33 Malware Investigation Task Forceの略。MITFは2007年5月から開始した活動で、ハニーポットを用いてネットワーク上でマルウェアの活動の観測を行い、マルウェアの流行状況を把握し、対策のための技術情報を集め、対策につなげる試み。

＊34 脆弱性のエミュレーション等の手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの取得検体数の推移を図-7に、マルウェアの検体取得元の分布を図-8にそれぞれ示します。図-7では、1日あたりに取得した検体[*35]の総数を総取得検体数、検体の種類をハッシュ値[*36]で分類したものをユニーク検体数として示しています。

期間中での1日あたりの平均値は、総取得検体数が371、ユニーク検体数が41です。前回の集計期間では、平均値が総取得検体数で378、ユニーク検体数で32でした。今回は、総取得検体数に減少傾向が見られますが、検体の種類を表すユニーク検体数が前回より増加傾向にあります。総検体取得数が9月19日以後急激に減少しているのは、世界中でSdbotとその亜種の活動が見られなくなったことによります。このSdbotの活動停止の原因は不明です。

図-8に示す検体取得元の分布では、日本国内が38.7%、国外が61.3%でした。なお、台湾が47.8%と前回に引き続き大きな割合を占めています。これは、台湾においてSdbotとその亜種の活動が活発であったためですが、他の国の状況と同様に9月19日以後は活動が見られなくなっています。

MITFでは、マルウェアの解析環境を用意し、取得した検体について独自の解析を行っています。今回の調査期間に取得した検体は、ワーム型14.0%、ボット型84.8%、ダウンローダ型1.2%でした。また、解析により、26個のボットネットC&Cサーバ[*37]と276個のマルウェア配布サイトの存在を確認しました。今回、マルウェア配布サイトの検出数が大幅に増加していますが、これは前回減少傾向が見られた複数の配布サイトにアクセスする検体が増加したためでした。

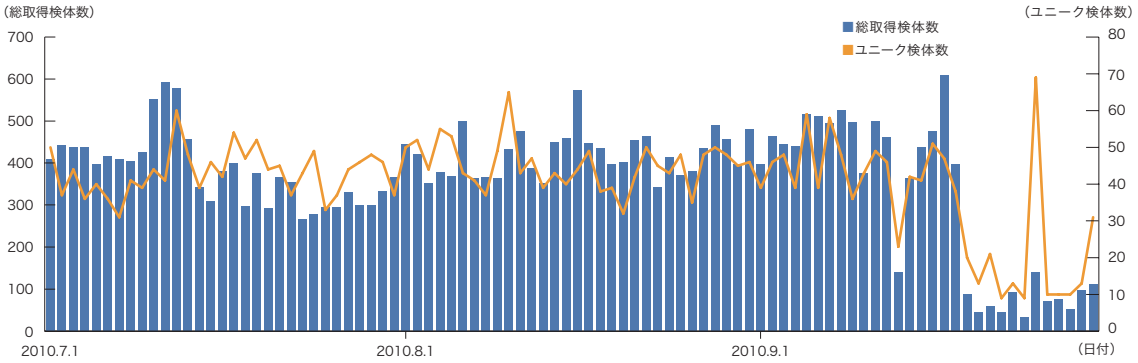


図-7　取得検体数の推移(総数、ユニーク検体数)

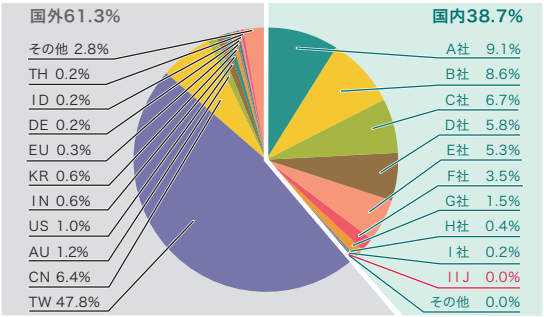


図-8　検体取得元の分布(国別分類、全期間)

＊35 ここでは、ハニーポット等で取得したマルウェアを指す。

＊36 様々な入力に対して一定長の出力をする一方向性関数(ハッシュ関数)を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディング等により、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮したうえで指標として採用している。

＊37 Command & Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃*38について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題になった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2010年7月から9月までに検知した、Webサーバに対するSQLインジェクション攻撃の推移を図-9に、攻撃の発信元の分布を図-10にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本40.0%、中国36.7%、米国7.1%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生状況は、前回からあまり変化が見受けられませんでした。しかし、9月30日に主に中国から特定の攻撃先に対しSQLサーバに侵入を試みる攻撃があったため、全体に対して中国からの攻撃が占める割合が増加しています。

ここまでに示したとおり、各種の攻撃はそれぞれ適切に検出され、サービス上の対応が行われています。しかし攻撃の試みは継続しているため、引き続き注意が必要な状況です。

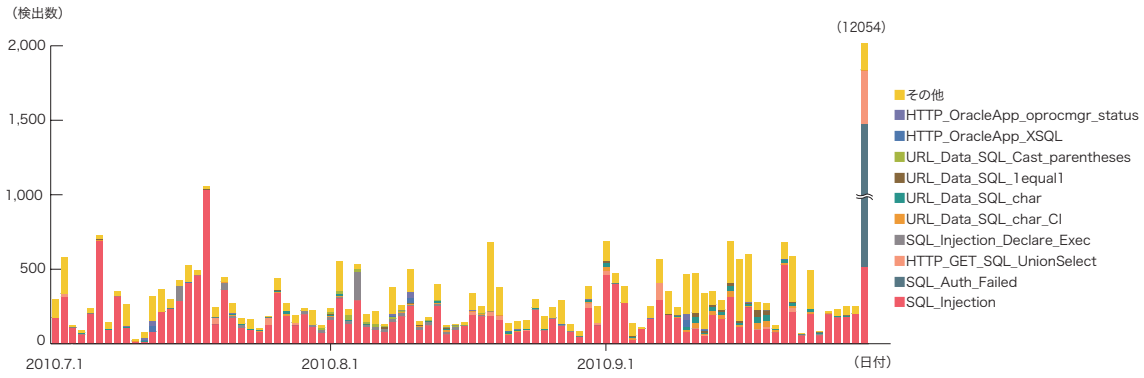


図-9　SQLインジェクション攻撃の推移(日別、攻撃種類別)

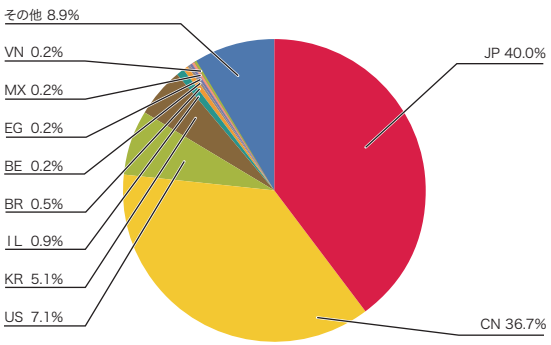


図-10 インジェクション攻撃の発信元の分布(国別分類、全期間)

＊38 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、小規模システムでのDDoS攻撃への備え、共用システムにおけるセキュリティ、デジタルフォレンジックの概要を示します。

1.4.1 小規模システムでのDDoS攻撃への備え

「1.3.1 DDoS攻撃」に示した通り、本レポートの対象期間の9月に複数のWebサーバへのDDoS攻撃が発生しました。この攻撃では、日本の官公庁に加えて民間企業のWebサーバ等も攻撃対象になりました。この事件に限らず、DDoS攻撃は攻撃対象のサーバの所有者に対する抗議や自己主張の一つとして行われます。また近年では、DDoS攻撃を行いながら金銭を要求する恐喝事例なども発生しています。現在のDDoS攻撃には、専用の攻撃ツールやボットネット等が利用され、攻撃自体を代行する者も存在しています。つまり、攻撃の意図を持つ者に知識や技術がなくても比較的容易に攻撃が行える状態になっています。このため、インターネット上に公開しているサーバは、その規模の大小にかかわらず、DDoS攻撃の対象となる可能性があります。ここでは、特に小規模システムでのDDoS攻撃への備えについて検討していきます。

DDoS攻撃には、サーバ自体を直接過負荷にする攻撃と、サーバが利用している回線を通信で埋めつくす攻撃の2つがあります。しかし、どちらの攻撃も、インターネットに接続しているサーバが突然利用できなくなることに変わりはありません。攻撃発生時に有効となる対策を検討するためには、サーバの重要度に基づく対策方針の策定、サーバの耐性向上、異常検出の仕組みの構築、他組織への協力要請等の準備が必要です。

■ 対策方針の策定

DDoS攻撃を受けた場合、サーバはその役割を果たすことができなくなります（可用性に対する脅威）。このため、検討対象のサーバが停止したときに、業務にどのような影響があるかを明らかにします。その上で、サーバの機能の回復目標を定めます。例えば、全面停止していても問題のないシステムなのか、通信できる範囲を特定の領域（日本国内や業務上の提携相手のみ等）に限定しても構わないのか、通信の品質を下げて（特定のアドレスからの接続数を制限したり、全体に帯域制御をかけたりして）も問題にならないか、といったことを検討します。どうしても可用性が求められるサーバについては、専用のDDoS対策装置の導入や対策サービスの利用を検討します。

■ サーバの耐性向上

DDoS攻撃を受けたときには、回線が通信で埋めつくされたり、サーバが過負荷状態に陥ったりします。このため、無防備なサーバでは、通信状況を確認したり、サーバの動作状況を確認したりすることさえ困難になります。サーバの導入時には、通常の業務で要求される処理能力を検討し、その状態に対してある程度の余裕を持たせることが必要です。あわせて、サーバのOSやアプリケーションでのDDoS対策や資源管理のオプションの導入を検討しておくことも大切です。例えば、

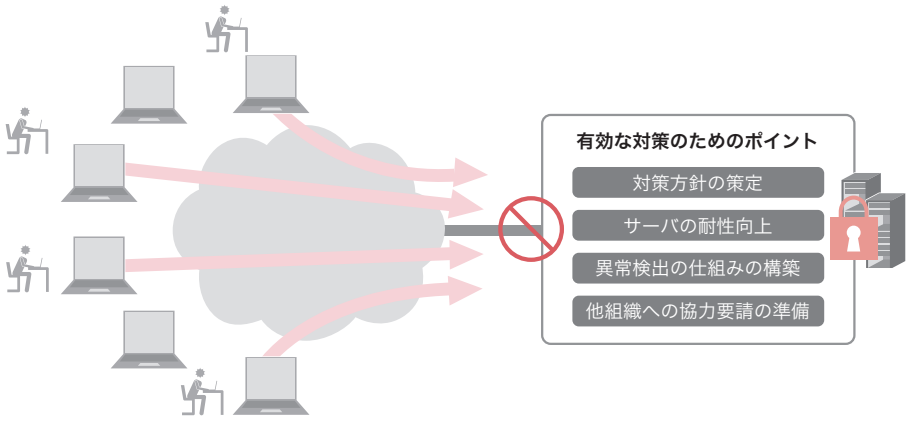


図-11 DDoS攻撃に対する準備

Linuxには、SYN flood攻撃を防御するSYN cookiesの機能[*39]や、アプリケーションごとに接続数を制限する機能[*40]等が搭載されています。HTTPサーバのApacheでも、設定[*41]や各種外部モジュール[*42]を追加することで、同時接続数等を制限する機能が利用できます。このようにハードウェアの性能と、OSやアプリケーションの機能を組み合わせることで、DDoS攻撃に対するサーバの耐性をより強固にすることができます。

■ 異常検出の仕組みの構築

DDoS攻撃を受けた場合に状況を把握しようとしても、日常的に適切なログを取得していなかったり、膨大な量のログを扱わなければならなかったりするため、解析を終えるまでに非常に長い時間がかかる場合があります。このため、日頃から適切なログの記録と通常の通信状態の把握を行い、突発的に発生するDDoS攻撃を異常として検知する仕組みを備えておくことが重要です。また、サーバのログだけではなく、SNMPやNetflow等により通信に関する情報も参照できるようしておくことで、より状況を把握しやすくなります。さらに、大量のログを取り扱うための準備も必要です。例えば、Webサーバとは別にログサーバを用意しておくことで、Webサーバが過負荷な状況でも記録を分析することができます。また、事前に大量のログから概要情報を抽出するスクリプト等を準備しておくことで、異常を検知した時に短時間で状況を把握できます。

■ 他組織への協力要請の準備

回線を通信で埋めつくしたりIPアドレスを詐称したりする攻撃では、攻撃を受けたサーバだけで対処できず、ISP、セキュリティベンダ、CSIRT等の外部組織に対処の協力要請を行うことが必要となる場合があります。この際には、すでに把握している状況を開示することが必要です。また、多くの場合、協力を要請した組織だけでは対策が行えず、攻撃に関する情報を他の組織（攻撃者を収容するISP等）と共有する許可を与える必要もあります。IPアドレス、攻撃の内容、通信の様子等、攻撃に関する個々の情報の開示の可否を事前に定めておくことで、他組織が迅速に対策活動を行えるようになります。このような情報については、JPCERT/CCのインシデント報告フォーム[*43]等が参考になります。

■ まとめ

ここでは、小規模システムを対象にして、DDoS攻撃を受ける前に備えておくべき事柄について説明しました。「1.3.1 DDoS攻撃」のbackscatter観測で示しているように、現在ではWebサーバ以外のサーバに対するDDoS攻撃も観測されており、あらゆるサーバで突然のDDoS攻撃に備えておく必要があります。また、DDoS攻撃は、攻撃者の意図が強く表れるものであり、その発生をある程度予見できます。このために、世間の動向や、所属する組織に関する情報等の自社のかかわるニュースにも注目し、諍いの前兆を早期に発見することも、DDoS攻撃への備えとして役立ちます[*44]。

1.4.2 共用システムにおけるセキュリティ

現在、クラウドコンピューティング（以下、クラウド）の本格的な利用が活発化しています。クラウドでは、さまざまなシステム資源を共用することで、それらを低コストで利用できる反面、共用システム特有のセキュリティに関する問題が懸念されています。ここでは、システム資源の共用から生じるクラウドでの脅威とその対策を検討します。

■ 共用資源における問題

マルチテナントでシステム資源を共用するクラウドでは、利用者間の資源の分離はソフトウェア等により論理的に行われます。このため、論理的な資源の分離が

＊39 SYN cookiesについての詳細は考案者であるダニエル・J・バーンスタインによるSYN cookiesの解説（http://cr.yp.to/syncookies.html）を参照のこと。また、IETFからSYN flood 攻撃についての攻撃原理と対策技術の概要をまとめた文書としてRFC4987 TCP SYN Flooding Attacks and Common Mitigations（http://www.ietf.org/rfc/rfc4987.txt）が発行されている。

＊40 iptablesではlimitやconnlimit等のモジュールが用意されている。例えばiptablesでlimitを利用しsynパケットに制限を加えることでアプリケーションが処理可能な新規接続数を絞るといった設定ができる。

＊41 例えば、MaxClientsの設定で同時接続数に制限を行える。これ以外にもTimeout、KeepAlive、KeepAliveTimeout、MaxKeepAliveRequests等がありこれらの設定を調整することで攻撃によるリソースの消費を抑制することができる。

＊42 Apacheには多くの外部モジュールが用意されており、例えば、mod_limitipconn（http://dominia.org/djao/limitipconn2.html）では1つのIPアドレスからの同時接続数を制限することができる。

＊43 詳細については次のJPCERTコーディネーションセンターのインシデントの報告（http://www.jpcert.or.jp/form/）を参照のこと。

＊44 その他、DDoS対策で参考となる情報としては例えば、VeriSign, Inc.：DDoS Mitigation - Best Practices for a Rapidly Changing Threat Landscape Whitepaper(要ユーザ登録)（http://www.verisign.com/forms/ddosbestpracticeswp.html?toc=MYUM9-0000-02-00）等がある。

適切であることが大変重要であり、分離している境界が破られることは利用者にとってセキュリティ上の脅威になります。では、実際にどのような脅威が考えられるでしょうか。CSA (Cloud Security Alliance) [*45] は“Top Threats to Cloud Computing V1.0” [*46] において、クラウドの代表的な脅威として7つの項目を挙げています。この7項目の中には、“Shared Technology Issues”という項目があり、CPUやGPUといった共用資源の論理的な分離や分割での違反の事例と影響が紹介されています。また、CSAのレポート以外にも、クラウド特有の脅威として、共有資源の問題が多くのレポートで取り上げられています。さらに、クラウドでは、通信回線や通信機器、ストレージといった資源も共用されるため、これらについても考えなければなりません。ここでは、クラウドのシステム構成を考慮しながら具体的な脅威について考えていきます。

■ クラウドのインフラストラクチャ構成

一般的に、クラウドの構成は公開されていません。このため、ここでは汎用的な機器で構成されているものと仮定し、図-12のような機器で構成されたクラウドシステムを例にクラウドの脅威を考えていきます。

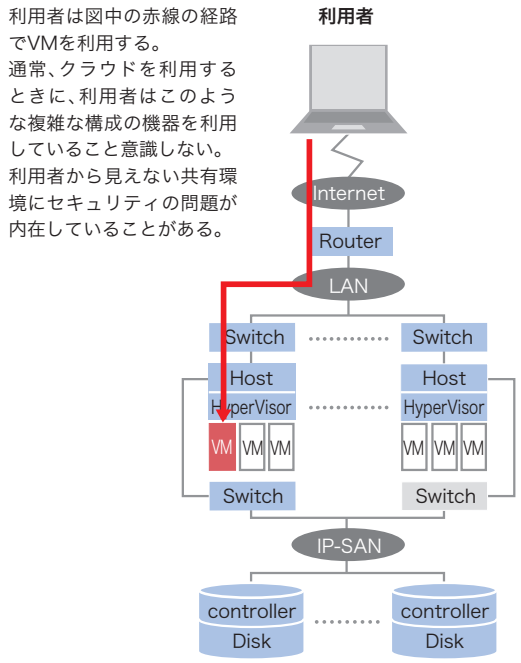


図-12 クラウドのシステム構成例

このクラウドはルータ等を使ってインターネットと接続しています。利用者はインターネットを通じてクラウド上の仮想マシン (VM) にアクセスします (図-12の赤い矢印)。仮想マシンが稼動している物理マシンには他の利用者の仮想マシンが同居しており、物理的な資源を共用しています。物理マシンはサービス提供のために複数のイーサネットポートをもち、インターネット側へのサービス提供や、イーサネットを使ったストレージネットワーク (IP-SAN) に接続されて、ストレージサービスを提供しています。

■ クラウド環境での脅威とその対策

ネットワークの共用は、クラウドだけに限られた話でなく、インターネット自体や、従来からのレンタルサーバ環境でも、複数の利用者がネットワークを共用しているという点で同一です。しかし、クラウドでは、異なるセキュリティポリシーの仮想マシンが同一のL2セグメント上に存在する可能性があります。仮想マシンが不正侵入によって乗っ取られ、ARP poisoning[*47]等により通信の阻害や盗聴が発生する危険性があります。このような脅威への対策として、ハイパーバイザーや、接続先のスイッチでVLAN ID、MAC Address等の詐称対策等を行うことが必要です。

また、クラウドでは、ストレージも仮想化され共用されます。IP-SAN (iSCSI) 等を利用している場合、イーサネットを使ってストレージが接続されるため、人為的に偽のイーサネットフレームを生成することでストレージネットワークを攻撃できます。仮想マシンから到達可能なネットワーク上にストレージのコントローラが存在する場合には、コントローラへの攻撃も可能です。また、ストレージ仮想化のためのID (IQN[*48]) が詐取されたときには、それによって本来は分離されていて、見えないはずのデータ領域が見えてしまったり

＊45 CSA(Cloud Security Alliance)。2008年にクラウドセキュリティのベストプラクティスを広めるために設立された団体(http://www.cloudsecurityalliance.org/)。2010年6月には日本支部として、日本クラウドセキュリティアライアンスが発足している(http://www.cloudsecurityalliance.jp/)。
＊46 “Top Threats to Cloud Computing V1.0”はCSAがクラウドコンピューティングへの代表的な脅威と対策をまとめて文書化したもの(http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf)。
＊47 ARP poisoningとはネットワーク上に偽のARPパケットを流すことにより、別のホストの通信を横取りする攻撃。
＊48 iSCSI Qualified Nameの略。ネットワーク上でiSCSIノードを識別するための名前。

接続できてしまったりする危険性があります。このような脅威への対策として、ネットワークと同様にハイパーバイザーやスイッチでのアクセス制御や詐称対策が必要となります。

さらに、ファイアウォール等の基本機能がサービスとして提供されている場合には、その提供形態によって脅威が変化します。図-13にファイアウォールの構成例を示します。パターン1は、ハイパーバイザーの一機能としてファイアウォールを提供する方法です。この場合、ファイアウォールの安全性は、事業者によって担保されます。パターン2は、利用者に提供される仮想マシンと同じように、ハイパーバイザー上にOSを載せ、ソフトウェアでファイアウォール機能を実現しています。この場合、ハイパーバイザーに脆弱性が存在していると、ファイアウォールもその影響を受けます。パターン3は、専用機器を用意し、VLANやルーティングでネットワークトラフィックを中継させる方法です。この方法は、従来のものと同じですが、コストがかかります。パターン4は、利用者のOS上に実装する方法ですが、不正侵入者によって設定が変更されてしまう危険性があります。パターン5は、Webやメールで用いられることが多い方法で、アプリケーションのproxy機能をSaaSとして利用する方法です。異なる事業者によってサービスが提供されているときには、サービス間の統制は利用者の責任になります。このように、提供形態によって考慮すべき点が異なることをあらかじめ認識しておく必要があります。

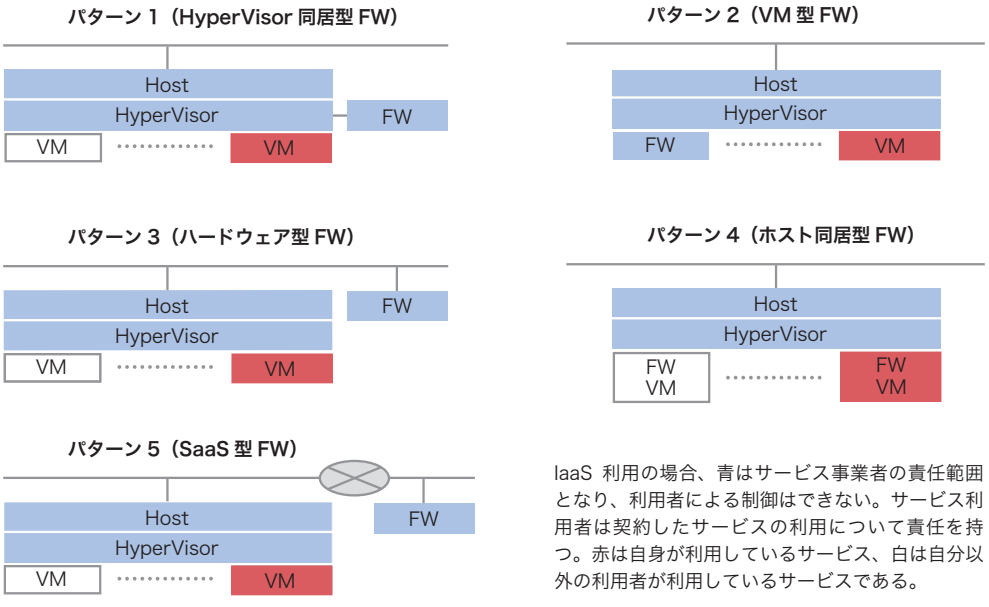
■ まとめ

ここで説明してきた事項は、目新しいものではなく、本来は事業者がそれぞれの脅威を認識して対策を行っていれば、問題になることはありません。

安全性を確認するために利用者自らが内部構成を意識することは有益ですが、サービス利用ではそのような情報が開示されないことも多々あります。利用者は、利用するサービスにおける利用者自身の責任範囲を見極めて必要な対策を行うことに加えて、事業者との間でセキュリティ対策に関する合意を形成していくことが、クラウドの利用において重要です。

1.4.3 デジタルフォレンジックの概要

ITが普及するに伴い、企業や個人が保持する情報の多くがデジタルデータとして保存され、蓄積されるようになっています。また、これによって、デジタルデータが事件の対応や裁判の証拠等に利用されるケースも増えています。デジタルデータは、紙媒体に比べると容易に変更したり消去したりできるため、それを調べる人には適切な技術が求められます。ここでは、デジタルデータの調査技術であるデジタルフォレンジックについて説明します。



IaaS 利用の場合、青はサービス事業者の責任範囲となり、利用者による制御はできない。サービス利用者は契約したサービスの利用について責任を持つ。赤は自身が利用しているサービス、白は自分以外の利用者が利用しているサービスである。

図-13 ファイアウォールの構成例

デジタルフォレンジックは、不正アクセス等を調査するインシデントレスポンス時や、訴訟における電子データの提出時等に、主に企業内で使われる技術[*49]です。解析対象の観点からデジタルフォレンジックを分類すると、コンピュータを対象にしたコンピュータフォレンジック、ネットワークを流れるパケットを対象にしたネットワークフォレンジック[*50]、携帯電話等のモバイル端末を対象としたモバイルデバイスフォレンジック[*51]等に分かれます。

また、デジタルフォレンジックの実施順序は、保全、解析、報告の3つのステップになります。デジタルフォレンジックでは、オリジナルのデジタルデータを使って解析することは、一部の例外を除いて基本的にありません。デジタルフォレンジックを実施するエンジニアは、最初に対象のデータを保全（複製、取得ともいう）する作業を実施します。次に、保全したデータを、そのデータに対応したツールで解析し、インシデント発生時の一連のイベントを可視化して再構築します。最後に、解析結果のデータを元に判明した事実を報告としてまとめます。

■ コンピュータフォレンジック

次に、実施頻度が高いコンピュータフォレンジックの保全と解析について説明します。

コンピュータは、CPUやメモリ、ハードディスク等によって構成されています。ハードディスクやCD-ROMに残っているデータは、コンピュータの電源を落としても消えることがない不揮発性のデータです。これに対して、CPUやメモリ上のデータは、電源を落とすと消えてしまう揮発性のデータです。 RFC3227 “Guidelines for Evidence Collection and Archiving”[*52]では、保全を実施する際には「揮発性の高いデータから順に保全する」ように推奨されています。したがって、調査対象のコンピュータがサーバであり、オンライン状態（電源が入っていて動いている状態）であったときには、まずメモリ上にあるデータ等の揮発性データを保全し、その後にディスクやその他のバックアップメディアを保全することが望ましいと言えます。

揮発性データの収集方法には、対象マシン上で揮発性データ収集ツールキットを実行する方法と、メモ

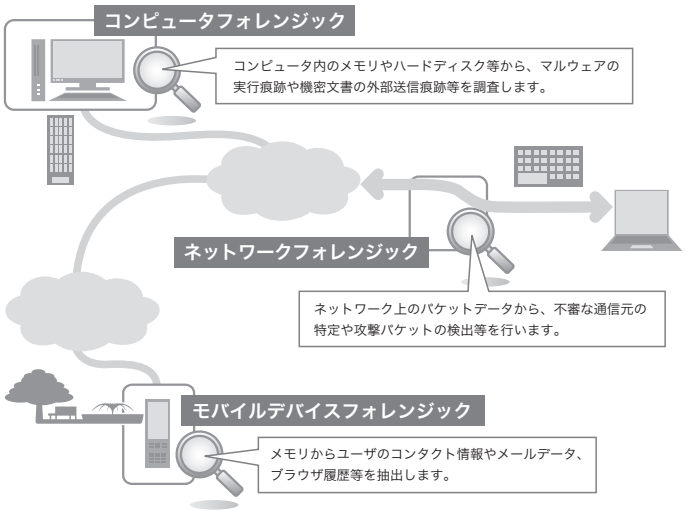


図-14 フォレンジックの概要

＊49 特定非営利活動法人のデジタル・フォレンジック研究会は、デジタルフォレンジックを「インシデントレスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」としている（http://www.digitalforensic.jp/wdfitm/wdf.html）。

＊50 遠隔から対象のコンピュータを調査・分析する手法をネットワークフォレンジックと呼ぶ場合もある。

＊51 モバイルデバイスフォレンジックについては、欧米で利用されているフォレンジックツールが日本の携帯電話の規格に対応していないため、法執行機関を除いて実施されることはほとんどなかったが、最近では徐々に増えてきたスマートフォンを対象としたツールを国内でも利用できるようになってきた。例えば、Oxygen Software社のモバイルデバイス解析ツールOxygen Forensic Suiteは、サイバーディフェンス研究所で取り扱っている（http://www.cyberdefense.jp/company_profile/prerelse10001.html）。

＊52 RFC3227 "Guidelines for Evidence Collection and Archiving" (http://www.ietf.org/rfc/rfc3227.txt)では、セキュリティインシデント発生時の証拠の収集手順や注意点を述べている。日本語訳にはIPAによる「証拠収集とアーカイビングのためのガイドライン」（http://www.ipa.go.jp/security/rfc/RFC3227JA.html）等がある。

リイメージを取得した後に解析する方法の2つがあります。例えば、揮発性データ収集ツールキットとしてはSysinternals Suite[*53]があります。このツール群は、対象のマシン上で実行され、その結果をテキストファイル等に出力します。一方、メモリイメージは、メモリの内容をそのままダンプしたバイナリファイルのことです。メモリイメージの取得には、対象のマシン上でメモリの内容をダンプするツールの実行だけを行い、その後にそのメモリイメージを別のマシンに移動して解析し、揮発性の情報を抽出します。メモリイメージの取得は、必ず揮発性データ収集ツールキットの実行よりも前に実施します[*54]。

不揮発性データの取得方法には、オンライン状態での保全とオフライン状態（電源を落とした状態）での保全の2つがあります。また、保存データの形式には、物理ディスク単位で保全する物理ディスクイメージや、論理ボリューム単位で保全する論理ディスクイメージ等があります。基本的に、不揮発性データはオフライン状態で保全します。ただし、ディスクが暗号化されていたりRAID構成が設定されていたりして、論理ボリュームで保全したほうが都合のよいときには、オンライン状態で保全することもあります。また、保全したデータは、保全後のデータの完全性を保証するために、保全時のハッシュ値を計算しておきます。これによって、保全後のデータが変更されたり改ざんされたりしても、それを検出できます。

保全した揮発性データを解析することで、ログオンしていたユーザの情報、実行中のプロセスの通信状態や開始時刻、プロセスがオープンしていたファイルや読み込んでいた共有ライブラリ、ARPテーブル、ルーティングテーブル、DNSキャッシュの情報等を得ることができます。また、メモリイメージファイルを解析することで、過去に実行されたプロセスの情報やすでにクローズした通信の情報等も得られる場合があります。

不揮発性データの解析で得られる結果は多岐にわたります。不正侵入時やマルウェア感染時には、関係する実行ファイルやログが隠ぺい目的によって削除されてしまうことが多いため、削除ファイルの復元を行ったり未使用領域内にあるログの断片を調べたりします。また、システムログやイベントログ、レジストリ等からインシデントに関係する操作やファイルを検出できれば、操作が行われた時刻や該当するファイルのタイムスタンプ（作成時刻や修正時刻等の情報）に近い別のイベントを調べていくことで、インシデント発生時期や被害範囲を推定することもできます。

さらに、揮発性か不揮発性にかかわらず保全したデータ内をキーワード検索することで、外部へのデータ送信痕跡を確認したり他システムへのアクセス有無を確認したりできます[*55]。

■ デジタルフォレンジックの課題

このようなデジタルフォレンジックにおける課題には、次のようなものがあります。

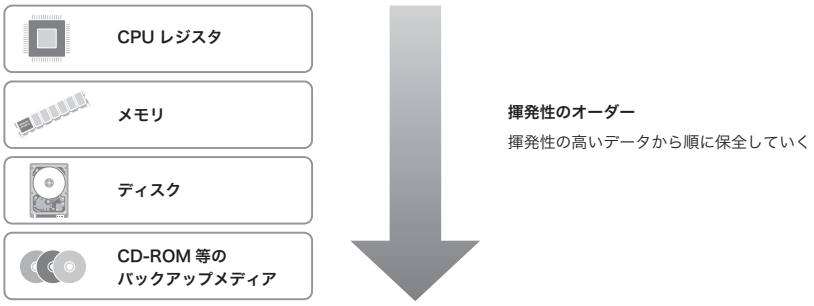


図-15 揮発性のオーダー

＊53 Sysinternals Suiteには実行中プロセスの情報を表示するPsListやTCP接続の状態を表示するTcpView等揮発性のデータを収集する多数のプログラムが含まれる（http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx）。

＊54 揮発性データ収集ツールキットは、数多くのプログラムで構成されており、それらの実行によるスワップ発生などで、メモリイメージの内容に影響を与える可能性がある。

＊55 ここで示したようなデータ解析を行うためのツールとしては EnCase（http://www.guidancesoftware.com/）、FTK（http://www.accessdata.com/）、TSK（http://www.sleuthkit.org/）等がある。

●複数ソースのログの集約
●アンチフォレンジックへの対応
●メディアの大容量化や暗号化への対応

複数ソースのログの集約に関する課題の例として、情報漏洩による機密情報の拡散範囲の調査があります。この場合には、コンピュータフォレンジックに加えて、ネットワークフォレンジックの実施も必要です。具体的には、ファイアウォール、ルータ、IDS等の各ネットワーク機器のログやパケットデータをコンピュータ側の情報と突き合わせる必要があります。しかし、各機器のログのフォーマットが異なっていたり、設定されている時刻にずれが生じていたとき等には、この突合せ作業は大きな負担となります。

アンチフォレンジックは、デジタルフォレンジックによる検出を逃れるための手法です。例えば、ファイルシステムのタイムスタンプを元に関係するファイルを調べていく手法から逃れるために、作成したファイルの時刻情報としてランダムな時刻をセットし直すマルウェアがあります。そのようなアンチフォレンジックに対しては、ファイルシステム以外のタイムスタンプ[*56]を活用する必要があります。

保全対象となるメディアのサイズも年々増大しています。できるかぎり短い時間でデータを保全するためには、保全する機器やソフトウェアの性能向上を待つしかありません。しかし、十分な時間を確保できないときには、保全前にプレビュー（対象のメディアを読み取り専用でマウントして直接調べる）を活用することも１つの手段になります。また、大容量のメディアを効率よく解析するためにプロセスを自動化できることも望まれています。加えて、最近ではメディアが暗号化されているケースも多く見受けられます。このようなときには、オンライン状態で保全するか、オフライン状態で保全した後に復号化する手段を確保しておく必要があります。

■ まとめ

デジタルフォレンジックをインシデントレスポンスに活用することで、重要な手がかりとなるデータを見逃すことなく、インシデントの発生原因やその影響範囲を調査することが可能です。IIJでは、今後もデジタルフォレンジックでの課題の解決方法を検討していくとともに、常に最新技術動向を調査しその知見を対応方法に取り入れていきます。

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、インシデント対応に必要な準備として、小規模システムでのDDoS攻撃への備え、クラウドコンピューティング等の共用システムにおけるセキュリティと、デジタルフォレンジックの概要を取り上げました。

IIJでは、このレポートのようにインシデントとその対応について明らかにし公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続してまいります。

執筆者:
齋藤 衛（さいとう まもる）
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、Webで感染するマルウェア対策コミュニティ等、複数の団体の運営委員を務めるとともに、安心ネットづくり促進協議会 児童ポルノ対策作業部会 技術者SWG、IPAサービス妨害攻撃対策検討会等においても活動も行う。

土屋 博英（1.2 インシデントサマリ）
土屋 博英 鈴木 博志 永尾 禎啓（1.3 インシデントサーベイ）
齋藤 衛 土屋 博英（1.4.1 小規模システムにおけるDDoS攻撃への備え）
加藤 雅彦（1.4.2 共用システムにおけるセキュリティ）
春山 敬宏（1.4.3 デジタルフォレンジックの概要）
IIJ サービス本部 セキュリティ情報統括室

協力:
須賀 祐治　吉川 弘晃　小林 直　齋藤 聖悟　IIJ サービス本部 セキュリティ情報統括室

＊56 他のタイムスタンプとしては、ファイル自身が内部に持つ情報や、ショートカットファイルが持つオリジナルファイルの情報、レジストリキーの情報等がある。Webブラウザやメール経由でのマルウェア感染時にはブラウザ履歴やメールの送受信日時等も手がかりになる。